CLAIMS:

1. A mobile terminal adapted to

receive a message via a mobile communications network;

request authentication data from the user of said mobile terminal; and transmit said authentication data to an authentication system for authenticating the user of said mobile terminal.

2. A mobile terminal according to claim 1, further being adapted to automatically generate an acknowledgment message to the sender of said message.

3. An authentication system for transmitting information, said authentication system storing identification information of a plurality of providing users and a plurality of receiving users and being adapted to

receive information from at least one of said providing users;

authenticate said at least one providing user; and

transmit a message including said information via a mobile communications network to a receiving user's mobile terminal.

4. An authentication system according to claim 3, further being adapted to authenticate a receiving user as the recipient of said information.

5. An authentication system according to claim 3 or 4, further being adapted to

provide a public/private key pair valid only for a single communication between the authentication system and said receiving user,

wherein said communication comprises a message and/or a response to said message;

encrypt at least part of said message using said public/private key pair; and to

send said public key to said receiving user as part of said message.

6. An authentication system according to claim 3 or 4, further being adapted to

provide a public/private key pair valid only for a single communication between the authentication system and said receiving user;

wherein said communication comprises a message and/or a response to said message;

send said public key to said receiving user terminal prior to said communication and store said public key in said mobile terminal; and to

encrypt at least part of said message using said public/private key pair.

7. An authentication system according to any of claims 3 to 6, further being adapted to extract a public key specific to said receiving user

from said stored identification information and to use said further public key for encryption of said at least part of said message.

8. An authentication system according to any of claims 3 to 7, further being adapted to receive an acknowledgement message or a response message from said receiving user.

9. An authentication system according to claim 8, further being adapted to transmit a confirmation message to said one providing user based upon said acknowledgement or response message.

10. An authentication system according to claim 9, wherein said confirmation message requires an acknowledgement message from said one providing user and said authentication system further being adapted to send a confirmation message to said receiver user's terminal, notifying the terminal to decrypt and display the decrypted part of said message.

11. A method of transmitting a message via a mobile telecommunications network from a sender's device to a user's terminal, wherein the user is required to acknowledge receipt of said message in a predetermined way and an acknowledgement message is subsequently transmitted to the sender of said message.

12. A method according to claim 11, wherein said user is required to authenticate himself by providing authentication data.

13. A method according to claim 12, wherein said user's terminal automatically generates said acknowledgement message upon supply of said authentication data and/or response data.

14. A method according to claim 12 or 13, wherein a central authentication system verifies the user's authentication.

15. A method according to any of claims 11 to 14, wherein said message or a portion thereof is only displayed to the receiving user if the receiving user provides a valid authentication.

16. A method according to any of claims 11 to 15, wherein said message is a SMS message according to the GSM standard.

17. A method according to any of claims 11 to 16, wherein at least a portion of the text message is encrypted by the sender's device before transmission and decrypted by the receiving terminal before display.

18. A method according to claim 17, wherein the text message comprises a first portion including the body of said message and a second

portion containing encryption data used for encryption of said body and required for decryption of data included in said body.

19. A method according to claim 18, wherein said second portion is unencrypted.

20. A method according to claim 18 or 19, wherein authentication data provided by the receiving user and/or response data to said message are encrypted using said encryption data.

21. A method according to claim 18, 19 or 20, wherein said encryption data are valid only for a single communication between the sender and the receiving user, said communication comprising said message and a response to said message.

22. A method according to any of claims 18 to 21, wherein said encryption requires further encryption data stored in the sender's device.

23. A method according to any of claims 18 to 22, wherein said decryption requires further encryption data stored in the receiving terminal.

24. A method according to any of claims 11 to 23, wherein at least a portion of said message and/or response message to said message is

automatically deleted after a predetermined time period from said mobile terminal.

25. A method according to any of claims 17 to 24, wherein authentication data are used for encryption and decryption of said portion of said message.

26. A method according to any of claims 11 to 25, wherein conventional short message protocols and software applications running on the communications devices are used to implement the method.

27. A method according to any of claims 11 to 24, wherein in said sender's device and in said receiving user's terminal a transaction reference counter is implemented and wherein each of said transaction reference counters is incremented if a message is successfully received.

28. A method according to claim 27, wherein a transaction reference is included in every message transmitter from the receiving user to the sender.

29. A method according to claim 28, wherein said sender compares the received transaction reference with its transaction reference

counter and the sender only responds if the received transaction reference matches the sender's transaction reference counter.

30. A method of transmitting a text message via a mobile communications network, wherein a portion of said text message is encrypted using a private/public key pair, wherein said public key is valid only for a predetermined number of text messages.

31. A method according to claim 30, wherein said public key is transmitted in said text message.

32. A method according to claim 30, wherein said public key is transmitted in a text message, which is transmitted prior to said text message.